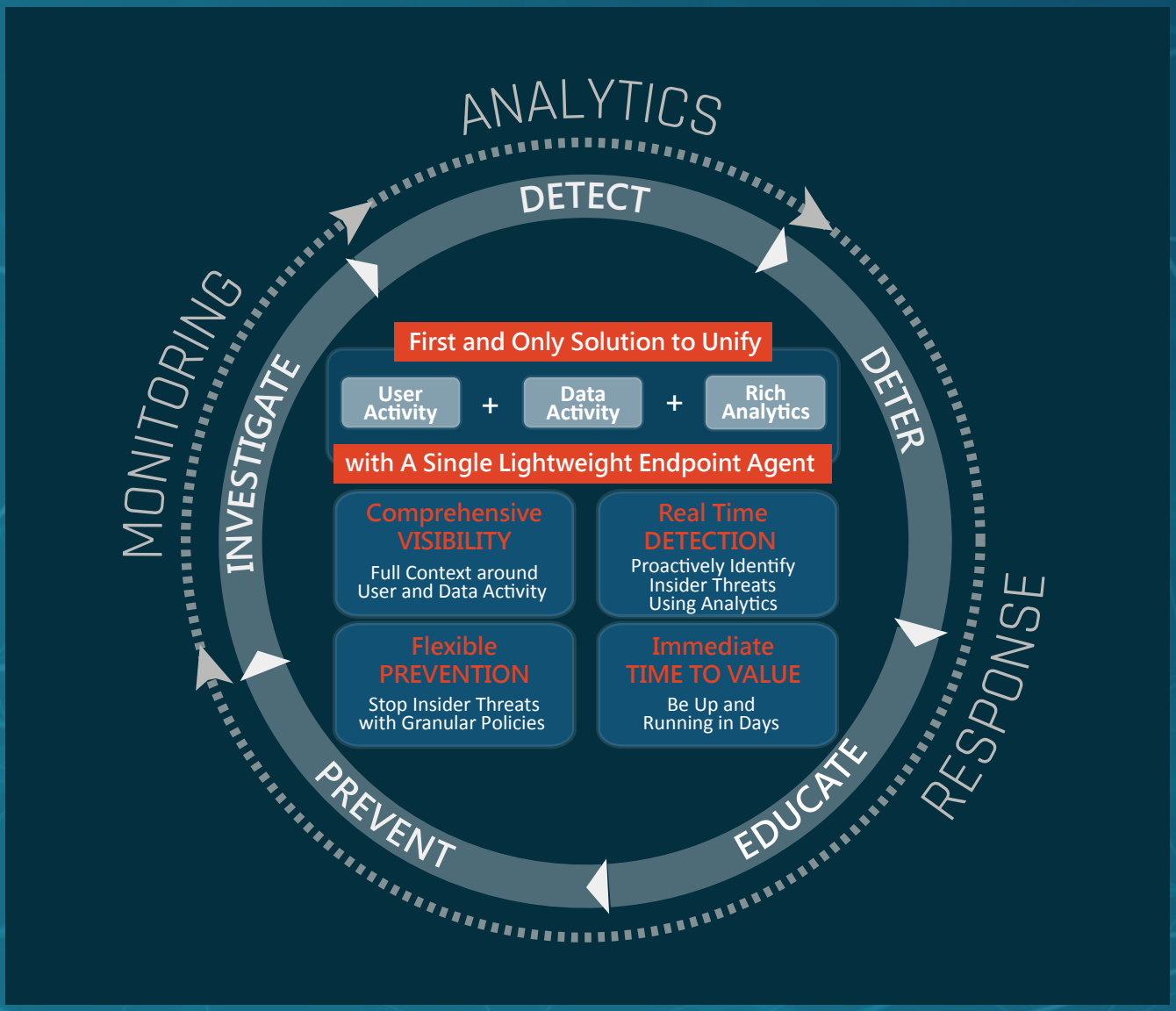
observe it

DETECT AND PREVENT INSIDER THREATS

智慧型視覺化內部威脅暨資料外洩防護解決方案



Complete **Context**:

Who. What. Where. When. Why.

台灣區授權總代理 | 漢領國際有限公司

ObserveIT - Know the Whole Story!

國際知名研調機構 Verison 於 2019 年 5 月底所發佈之年度資料外洩調查報告「Data Breach Investigations Report, DBIR」指出，全球因資料外洩而導致有形資產損失的產業排名依序為：公家機關、醫療業與金融業；事故發生原因多達 34% 源自內部人員使用行為不當有關。以下幾項為特別值得關注之名列前茅的統計：

1. 網路釣魚為入侵手法排名第一。 2. Email 為資料外洩最常發生之管道。 3. Microsoft Office 為資料外洩最多的檔案類型。 4.「人」是最佳攻擊目標。

ObserveIT v7.8 - email日誌功能 提升資料外洩防禦範圍與事件還原之完整性

全球最佳內部威脅管理解決方案 ObserveIT 自問世以來聚焦以「人」為導向的資安防禦，有效防範使用者行為所導致的資安事件與商業損失。就功能面，ObserveIT 鎖定細膩與精確的 User Activity Metadata 與 Analytics 作為持續研發藍圖，而應用面，則以內部威脅為核心主軸不斷深化與擴展。

ObserveIT 於 2017 年 Q3 正式推出 v7.1 版，即進化為涵蓋 User Activity + Data Activity + Analytics 三合一的內部威脅管理解決方案，積極強化「偵測」與「回應」能力，提供更高的內部威脅與風險可視性，並全力開發 DLP-like 的資料外洩防禦功能，以「人」、「流程」、「技術」三面向持續精進，將防禦時間軸往前提，提前洞悉資料外洩的關聯性並阻絕各類威脅使用行為。ObserveIT 專事各類使用行為之偵測分析，藉由行為實際畫面記錄及詳盡 Log 輔助，協助管理者將防禦時間軸提前，提早洞悉、預防與阻絕各類威脅使用行為與資料外洩的可能性。

ObserveIT 自 v7.0 版積極持續開發 FAM（File Activity Monitoring）相關功能，強化檔案日誌歷程追蹤軌跡，主動偵測內部檔案異常使用行為，如：大量檔案複製、雲端上傳 / 下載、Webmail 瀏覽、異常列印、檔案追蹤與檔名變更等。2019 年 Q1 推出 v7.7 版，強化 USB 檔案、Hotkey、Prtscn 及各類組合鍵之偵測，提供更細膩的事件還原完整性。

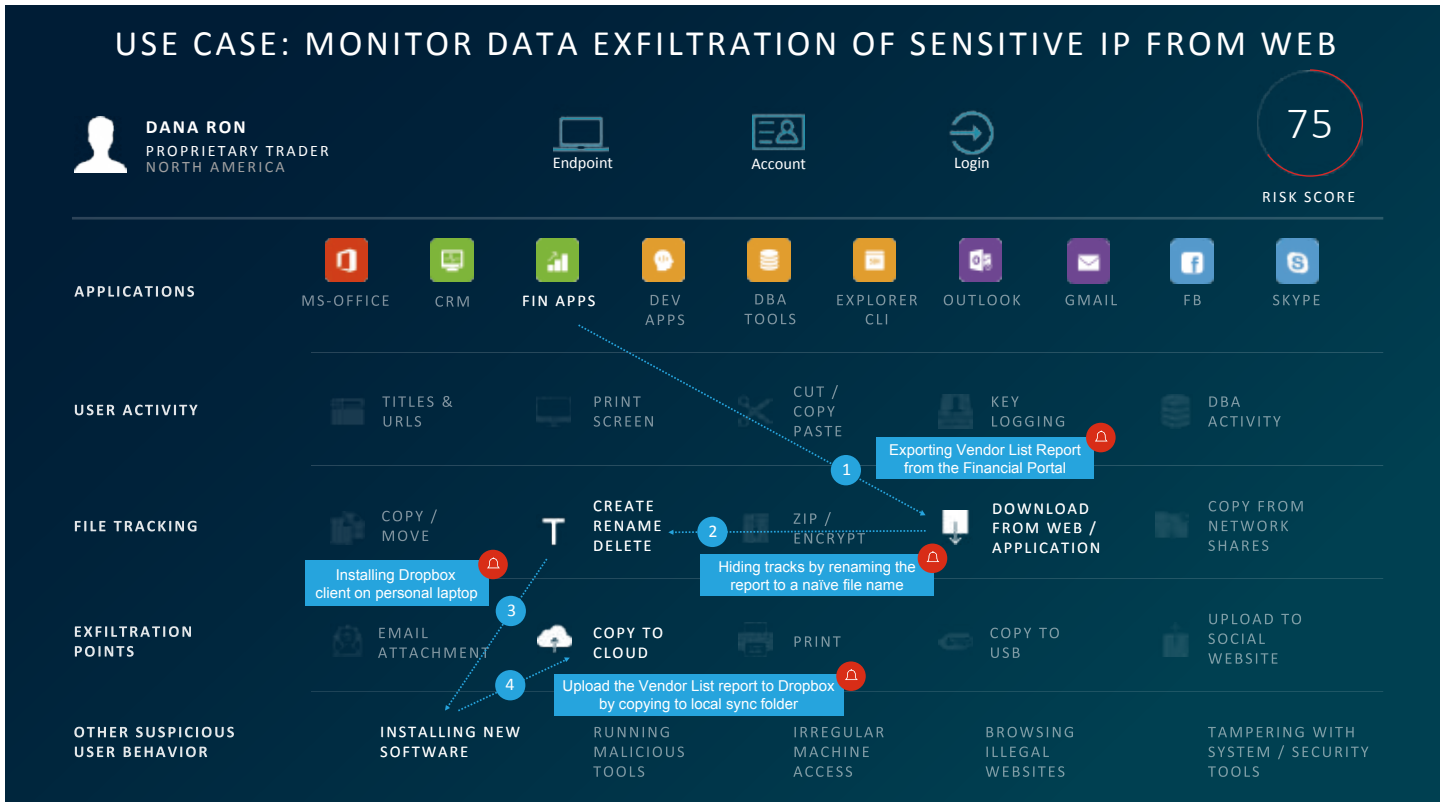
ObserveIT 2019 Q2 推出 v7.8 版，進一步強化資料外洩防禦範圍，增加 email 附檔資料外洩的監控偵測分析功能：

- 新增 email 偵測功能，包含 email 主旨、收 / 寄件人及密件副本欄位，email 附檔之檔名、檔案數量與檔案大小等。
- email 檔案完整歷程追蹤紀錄。
- 發送至非授權之 email 信箱時，可進行即時告警。
- 活動歷程回播（Activity Replay）可設定告警觸發前後之側錄方式與時間長短，有效降低所需之磁碟空間。
- 側錄工作階段增加端點當地時間戳記，強化全球化營運企業組織管理。
- 觸發告警規則設定亦增加調校功能，提升告警之精準度。

ObserveIT 功能特色

1. Web-Based風險儀表板提供管理者整體內部威脅可視性與關聯性，明確顯示各類使用者、部門單位、觸警風險行為累計/新增之指數與趨勢，並可自訂或套用內建逾320種告警規則/逾29種分類，以進行風險指數分析。
2. 提供使用者行為歷程進階統計分析，包括遠端連線來源、常用登入帳號/端點/裝置/應用程式/網站等分析與使用時間、平均活動或超時工作統計等。
3. FAM (File Activity Monitoring) 檔案活動監控功能，詳細的檔案日誌與使用歷程，凡檔案複製、移動、重新命名、刪除、上傳或下載等，皆可立即告警與追蹤視覺化檔案軌跡，加速數據資料外洩事件之調查。
4. Windows環境可進行應用程式進階控管，針對未授權或異常應用程式使用行為進行偵測，具備強制關閉未授權之應用程式或強制登出等預防機制。
5. 針對Linux環境可阻絕未經授權指令、指令參數或蛙跳行為，可偵測與側錄Linux/Unix使用者執行之命令與輸入指令後的Output字串，包括Script中內含之指令與系統命令產生的底層指令，及所有終端螢幕之輸出畫面。
6. Key-Logger功能完整記錄Windows/Mac鍵盤輸入及組合鍵，如：PrtScr、Alt-PrtScr、Ctrl-V、Cmd-Shift-3、Cmd-V等。
7. 可偵測 USB 儲存設備、SD Card 、iPhone、Android 行動裝置之序號、廠牌名稱、型號名稱等辨識，並建立黑白名單。當偵測到以快捷鍵複製或拖拉檔案至黑名單儲存設備時，將告警並紀錄資料外洩完整過程。
8. 針對列印工作進行監控、偵測與記錄印表機的列印工作細節，顯示使用者、主機名稱、印表機名稱/品牌、列印檔案名稱、列印頁數與大量列印等資訊。
9. 具備Email的監控功能，包含email的主旨、收/寄件人及密件副本欄位，夾檔之檔名與檔案大小等。
10. 具備URL安全過濾機制，內建逾數十種分類及逾數百億筆Indexed URLs情資資料庫並可每日更新，針對釣魚、高危險性、未被授權網站等之瀏覽行為進行偵測、告警或中斷。
11. 可設定「匿名模式」，將風險儀表板及 Web Console 所顯示之使用者資訊加以匿名，確保使用者隱私與個資之保護。
12. 側錄資料皆具備AES加密保護與浮水印，並具備雙重密碼保護機制亦可整合數位簽章，並須依管理權限以ObserveIT播放器進行回播，確保資料無法竄改同時提升證據能力。
13. Agent符合FIPS國際標準。具備離線側錄功能，網路斷線時Agent仍持續側錄，待連線恢復自動回傳檔案至資料庫。凡蓄意更改、刪除Agent檔案或終止Agent運作時，Agent之Watchdog機制將自動重啟並發送即時警示email通知管理者。
14. Agent支援Windows、Mac、Linux、Unix/HP-UX、Solaris等平台，Windows/Linux管理者身份或共用帳號可增設第二道認證並可與AD整合，及Windows身份盜竊偵測與警示功能。
15. 支援 VMwareView / RDSH、Citrix XenApp / XenDesktop、Ericom Connect、Windows Remote Desktop、Team Viewer、PCanywhere、VNC、Telnet、SSH、Netop、Dameware、Putty、WinSCP、SFTP等遠端連線操作側錄。
16. ObserveIT 之 Metadata / 告警事件提供 Database API、Restful API、CSV / CEF log 供外部 SIEM進行即時收容及分析。亦提供 Webservice 整合 Ticketing 系統，如 OITicket 工單申請覆核流程系統，以進行工單申請、核准及權限開通與視覺化覆核。

ObserveIT內部威脅偵測分析應用範例 - 資料外洩歷程軌跡

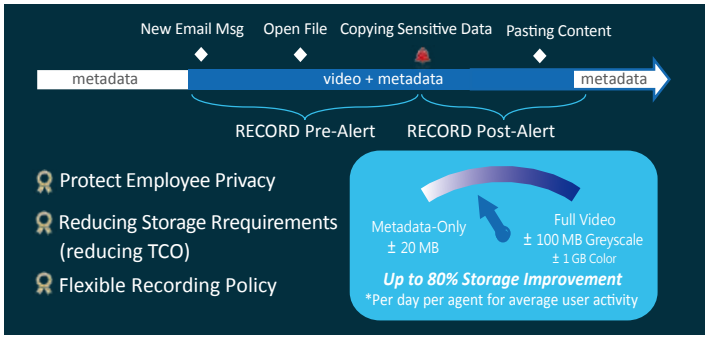


內建逾320種告警規則/逾29種內部威脅分類，進行偵測、阻絕、告警、側錄，可匯出風險使用行為分析報表

DLP範例項目	ObserveIT應用 – 偵測、告警、阻絕及視覺化側錄
上傳檔案至外部雲端平台及應用程式	雲端空間 – Dropbox、Box、Google Drive、iCloud。 Office365、OWA、Gmail、Webmail 等。
於內部機敏資訊平台上傳/下載檔案	內/外部Portal，如：醫療網、網路銀行、企業SharePoint、Salesforce、CRM 等。
可卸除式儲存裝置使用監控	偵測可卸除式儲存裝置廠牌、型號、序號及標籤。 偵測下載至可卸除式儲存裝置檔案之軌跡與來源。 建立可卸除式儲存裝置黑白名單及告警規則。
Email 資料外洩防禦及監控	寄/收件者郵件地址、主旨、夾檔之可視性。 網域名稱、檔案大小之黑名白單監控政策。 郵件夾檔上傳來源及下載後歷程追蹤。
檔案列印、複製/貼上	非上班時段大量列印、複製/貼上。 未授權檔案列印、複製/貼上、滑鼠右鍵貼上 ...。
Key-Logging告警/偵測/控管	鍵盤特殊功能鍵、組合鍵 - PrtScr, [Alt-PrtScr], [Cmd-Shift-3] , CTRL-V, CMD-V。
複製/貼上機敏文字	複製/貼上疑似信用卡號碼。 複製/貼上機敏檔案內文字。
存取未授權資料夾及檔案	存取未授權資料夾。 存取未授權UNC路徑。
執行惡意/駭客工具	使用惡意工具之即時告警：Nessus、Netsparker、Maltego等。
執行圖像隱碼術工具	使用隱碼術工具之即時告警：xiao_steg、camouflage 等。
於Linux/Unix系統執行檔案傳送指令	偵測Linux傳送指令，如：tftp、scp、rsync、GET。
使用P2P工具	偵測P2P 工具使用。

Web-Based 管理介面支援中英日韓德等多國語言，具備https加密連線

ObserveIT 風險行為分析報表



Activity Replay：可設定告警觸發前後之側錄方式與時間長短，如：觸發前後側錄方式為 Metadata + Video，一般時間則只側錄 Metadata; 亦可設定觸發前後側錄的時間長度，有效降低所需之磁碟空間。

全球87個國家近2,000家國際知名企業客戶青睞
持續獲得國際資安大獎肯定

Insider Threat Solution

Best Product Insider Threat Detection

End-point Security Management

Black Unicorn Awards

法規遵循與軌跡稽核

- 符合「個人資料保護法」、「金融機構辦理電腦系統資訊安全評估辦法」、「電子支付機構資訊系統標準及安全控管作業基準辦法」 等各項法規之遵循。
- 符合PCI、SOX、HIPAA、NERC、FFIEC、FISMA、FERPA ISO27001等國際法規遵循性，以及SWIFT國際組織CSP規範。
- 視覺化記錄內外部/遠端連線之使用者操作行為，同時提供詳盡的 Log 記錄，符合使用記錄、軌跡資料及證據保存之規範標準。
- 提供完整的AES加密視覺化記錄，提升證據能力及證據價值。

OITicket 工單申請覆核流程系統（額外模組）

提供Web-Based線上核准稽核4A機制，可與 Windows AD 整合以利快速建置上線使用，並以AD內建組織層級自訂核准流程，點選〝側錄畫面〞欄位可立即回播操作行為之加密視覺化記錄。

Authorization - 特權帳號工單申請核准及權限開通

- 統一內外部申請程序，可依資安政策與權限加以規範工單核准流程。
- 申請人可自訂作業期間、作業時段、伺服器、工作項目，並填寫工作描述，系統自動Email通知主管核准後，特權帳號之工單申請人方可登入伺服器執行核准之作業。
- 可依核准內容限制登入伺服器之作業期間及作業時段。
- 可防制蛙跳至後端其他未授權作業之主機。

Authentication - 工單流程記錄

- 集中保存申請記錄。
- 工單申請人依工單所核准之作業期間/作業時段內進行登入，未經核准之帳號或時段則不得登入。申請人工作完成後可自行回播並確認執行之內容，亦可列印執行結果之畫面。

Auditing - 視覺化線上稽核

- 稽核與相關主管可隨時檢視申請人執行內容畫面，並對工單記錄予以覆核。
- 各層級主管針對「待覆核」之工單，可於檢視歷程或回播後，標示為「勾選為已覆核」，若認為作業內容未完成或不符合申請，主管亦可將工單變更為「失效」。

Alert - 即時警示通知

- 可依執行應用程式、視窗標題、登入帳號、用戶端、時段等規則發送即時Email警示予管理者。

ObserveIT Agent 支援版本

Windows :
- 32/64-bit Windows 7/8/8.1/10 Windows Server 2008/2008 R2
- 64-bit Only Windows Server 2012/2012 R2/2016

Linux :
- RHEL/CentOS 5.10-5.11 & 7.0-7.6 x86_64, 6.7-6.9 & 7.0-7.4 x86_64/ppc64
- Oracle Linux 5.10-5.11, 6.7-6.9, 7.0-7.4
- Ubuntu 12.04 , 14.04, 16.04, 18.04 (LTS) i386/x86_64
- SLES SuSE 11, SP2-3, 12 i386/ x86_64
- Debain 7 ,8 & 9 (32/64-bit)
- Amazon Linux AMI 2015.03, 2017.09

Mac OS :
- Sierra 10.12
- High Sierra 10.13
- Mojave 10.14

IBM :
- AIX 6.1/7.1/7.2 32/64 bit

HP :
- UX 11.31 (Itanium 64 bit)

Solaris :
- X86/x64 or Sparc 10 update7-update11 11 update1-update3

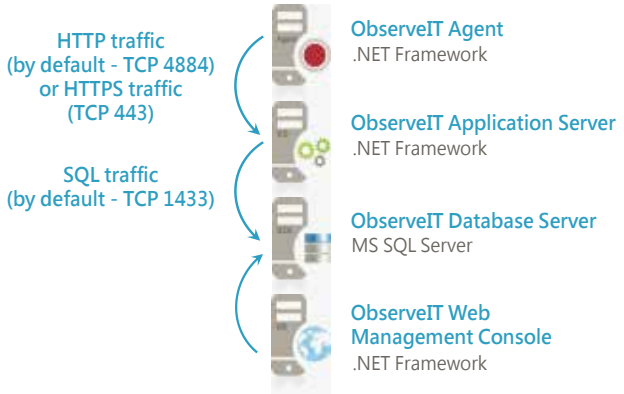
Virtual Desktop :
- VMware View
- Citrix XenApp/XenDesktop 5.x, 6.x,7.x (支援最高版本7.15)

ObserveIT Application Server & Web Console

Windows :
- 64bit Windows Server 2012/2012R2/2016
- IIS 8.0 with ASP.NET .NET Framework v4.5

ObserveIT Database

Windows :
- 64bit Windows Server 2012/2012R2/2016
- MS SQL Server 2012/ 2014/2016/ 2017 with latest Service Pack



observe it 授權台灣區總代理

漢領國際有限公司 JAS Lead

10682 台北市大安區敦化南路二段77號8樓之2
電話：+886-2-2709-6983
傳真：+886-2-2707-6983
www.jas-solution.com sales@jas-solution.com